Chief Information Officer
National Institutes of Health
Department of Health and Human Services

NIH Wireless Network Policy

October 8, 2002

Table of Contents

1. Purpose

This document establishes the policy for the deployment and use of wireless network technology at the NIH. It intends to protect NIH resources and data from security threats, improve incident response for wireless issues, and mitigate interference among wireless technologies.

2. Background

Wireless network devices offer a simple, convenient, and inexpensive solution to extend network accessibility by reducing the requirements of physical infrastructure. Wireless networking removes the encumbrance of wire connections on portable devices, and can also enable laptop and handheld users the ability to travel beyond traditional network boundaries (e.g. between buildings) without losing network connectivity.

In additional to the inherent risks associated with any wired network, wireless technology introduces several unique vulnerabilities. Since wireless signals are radio transmissions, they can be intercepted by suitable radio receiving devices, sometimes even devices operating outside the intended service area. If data transmissions are not encrypted or are inadequately encrypted, the intercepted data can be read and understood in a matter of seconds. Any data transmission sent through the wireless network is at risk, including research correspondence, usernames and passwords, financial data, and other sensitive information. Because wireless transmissions circumvent traditional perimeter firewalls, those existing protections established to prevent unauthorized access are ineffective. Advances in wireless signaling technology may increase transmission distances, further exacerbating the problem of unauthorized reception.

Exposure of sensitive data is not the only concern for the NIH. If improperly implemented, a wireless network allows an unauthenticated user an NIH IP address with all the benefits offered to any authenticated user. Using one of these trusted IP addresses, attacks could be launched against the NIH or any outside network accessible through NIHNet. Web sites devoted to open access points throughout the country are expanding and may eventually include open access points (“hot spots”) within the NIH.

Since wireless network devices operate using radio signals, their proliferation at the NIH can lead to Radio Frequency Interference (RFI) among these devices and other radio devices using the same frequency bands.

This policy serves as the foundation for a comprehensive risk mitigation strategy; enhanced by published security standards, best practice documents and, where applicable, more granular IC-specific policy.

3. Scope

This document establishes policies for wireless network access services implemented within the NIH. It applies to all NIH personnel, contractors and visitors that have access to NIH facilities

or NIH information. It applies to all wireless network access devices and technologies that provide a bridge between wireless and wired networks (hereafter "access points"), or any device that is designed to communicate with such a device via the wireless network (hereafter "access clients").

4. Applicable Policies and Guidelines

1) DHHS Automated Information Systems Security Handbook (AISSP) - http://irm.cit.nih.gov/policy/aissp.html

2) NIH Information Technology General Rules of Behavior - http://irm.cit.nih.gov/security/nihitrob.html

3) NIH Limited Authorized Personal Use of NIH Information Technology Resources - http://www1.od.nih.gov/oma/manualchapters/management/2806/

4) DHHS Policy for IT Security for Remote Access - http://irm.cit.nih.gov/itmra/HHS-IRM-2000-0005.html

5) NIH Remote Access Policy - http://www1.od.nih.gov/oma/manualchapters/acquisitions/26101-26-08/

6) Security Guidelines for NIH Remote Access Users - http://irm.cit.nih.gov/security/SecGui.html

7) NIH Password Policy - http://irm.cit.nih.gov/policy/passwords.html

8) NIH Warning Banner Policy - http://irm.cit.nih.gov/policy/warnbanners.html

9) CIT Guidance for Securing Data on Portable Systems - http://irm.cit.nih.gov/security/GuixSecuData.html

5. Policy

Registration of Wireless Devices

- All wireless network access points must be registered with a Central Wireless Device Database managed by CIT at the time of deployment in the NIH environment. CIT will provide a secure web interface for the IC ISSO or designated IC personnel to add, change and remove wireless devices on any NIHNet-connected network (including contractor sites).
- Registration of access clients is not required unless the same device is configured as an access point.
- CIT in cooperation with the IC ISSO will establish general risk mitigation strategies for access points, users and client devices such as virus protection, password standards and other preventative measures.

- Prior to deployment, access points must meet the standards of current security audits established by the CIT and the IC ISSOs and published in the "NIH Wireless Network Security Standards"
- Only approved and registered access points will be deployed within the NIH. Unapproved (rogue) devices may be removed from service by CIT in coordination with the IC's ISSO.

Management and Security of Access Points

- Physical Security: Access points should be properly secured within a safe, adequately monitored area to prevent unauthorized access and physical tampering. Devices should not be placed in easily accessible public locations.
- Configuration Management: All wireless access points must be secured using an administrative password per the password requirements in the NIH Password Policy. Administrators must ensure all vendor default usernames and passwords are removed from the device. Administration of the device should be prohibited from the wireless network.

Broadcast Security and Encryption

- CIT in coordination with the IC ISSOs will provide an updated standards list that will include approved wireless technologies, current minimum encryption standards, and best practices for secure installations. (See the "NIH Wireless Network Security Standards" document)

Access to NIH Facilities and Data

- Once authenticated to an access point, users must either be routed outside the NIH firewall(s), or authenticate to an NIH network. Just as with a wired network, NIH network authentication, whether NIH-wide or IC-specific, must satisfy prescribed login/password combinations prior to using NIH or IC-specific resources that are not normally accessible by nodes outside the NIH firewall(s).
- Access control mechanisms such as firewalls should be deployed to separate the wireless network from the internal wired network.
- As the technology permits, wireless networks should employ a combination of layered authentication methods to protect sensitive, proprietary and patient information.

Naming Conventions

- Final device names are assigned during the registration process to avoid conflicts and confusion, and to aid the IRT and IC ISSOs in identifying and locating wireless devices.
- If technology allows for the broadcast of a device name, standardized names shall appear in the broadcast description, along with any unique identifiers assigned to the unit.

Disruption and Interference

- All newly deployed wireless technologies must satisfy all existing and future standards as required by law or established by the NIH Spectrum Management Team.
- The NIH CIO in coordination with the ITMC will resolve any conflicts between wireless devices. Priority is granted to fully supported and registered installations except as appropriate in the case of medical, safety, or emergency devices.

6. Procedures

Registration process

At the time of deployment, all wireless devices will be registered with the Central Wireless Device Database. Registration information will include, but is not limited to, the following information:

- Contact information for owner and responsible parties
- Location of devices
- Intended use and coverage area
- Type of wireless technology deployed
- Manufacturer name and model number
- Device description
- SSID/ESSID (or equivalent)
- Hopping sequence (if applicable)
- Security checklist responses

Security Auditing and Intrusion Detection

Device installers must ensure the wireless device is properly secured prior to deployment. Once deployed, the responsible ISSO shall perform a security analysis using current wireless security methods. All wireless devices must meet the minimum security requirements dictated by NIH policies.

Incident Handling Process

Coordination between the IRT, IC ISSOs and other designated parties will follow existing and future guidelines available through the IRT Web site.
http://irm.cit.nih.gov/security/ih_guidelines.html

7. Roles and Responsibilities

The NIH Chief Information Officer (CIO)

The NIH CIO develops and implements NIH-wide policy for wireless devices and is ultimately responsible for the safety and security of the NIH Enterprise Network. The NIH CIO or designee must approve all exceptions to this policy.

The NIH IT Management Council (ITMC)

The NIH ITMC provides broad level oversight and guidance on NIH Wireless Policy and operations. The ITMC serves as the review and advisory body for the development and implementation of the actions required by this policy.

The NIH Senior Information Systems Security Officer (Sr. ISSO)

The NIH Sr. ISSO is responsible for ensuring the technical security of the NIH Enterprise Network. He/she is responsible for implementing this policy and providing the detailed monitoring, and enforcement tools and procedures.

The IC Chief Information Officer

The IC CIO is responsible for the overall control and supervision of each IC-specific wireless implementation, and is also responsible for IC compliance with this policy.

The IC Information Systems Security Officer (ISSO)

The IC ISSO is the IC's point of contact for receiving alerts and other notifications that result from the enforcement of this policy. ISSOs are responsible for enforcement of this policy within their respective ICs. ICs are encouraged to designate a specific e-mail address and phone number for 24 x 7 notification.

The NIH Incident Response Team (IRT)

The IRT, in cooperation with the IC ISSOs, will regularly scan the RF spectrum for vulnerable and/or unregistered wireless devices and will coordinate with IC ISSOs in the event of a possible system compromise.

Spectrum Management Team

The Spectrum Management Team is responsible for maintaining the list of acceptable RF frequencies and wireless technologies. It will conduct periodic spectrum analysis to assess the potential impact of electromagnetic interference (EMI) from transmitters and the impact of electromagnetic emissions from wireless devices.

CIT TASC

CIT's Technical Assistance Support Center provides educational resources and instructional materials to support the deployment of wireless technology within the NIH.

8. Information and Assistance

Comments, questions, suggestions or requests for further information should be directed to the NIH Sr. ISSO at (301) 402-4457.

9. Effective Date/Implementation

The effective date of this policy is the date the policy is signed by the NIH CIO**.**

10. Approved

_____/s/_____
Alan S. Graeff DATE: October 8, 2002
Chief Information Officer, NIH

Glossary

NIH Firewall – The NIH firewall is a network device used to block unauthorized network traffic from entering NIHnet.

NIHnet – NIHnet is the name used to designate the NIH backbone computer network and all subnetworks attached to the NIH backbone.

Sensitive Data – Sensitive data are data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction

of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

Service Set Identifiers (SSID) – A unique indentifier attached to the header of packets sent over a LAWN (Local Area Wireless Network). It is primarily intended to differentiate LAWNs, but also acts as a rudimentary password.

Wireless – A technology that permits the transfer of information (active or passive) between separate points using electromagnetic waves rather than a physical connection.